

Marine Corps University / Command and Staff College
Warfighting / Complex Operational Problem Solving and Design

Lesson Title: Planning for Cyberspace (& Space) Operations

Lesson: 6204 (AY-15)

Author: LtCol P. M. Melchior

Revision Date: 15 Nov 14

"A failure by the Department to secure its systems in cyberspace would pose a fundamental risk to our ability to accomplish defense missions today and in the future."
2010 Quadrennial Defense Review

"Never use a product designed to attack your freedom unless you personally have the means to defeat that attack."

Mr. Richard Stallman
Founder of Free Software Foundation

"We don't have a traditional strategy process, planning process like you'd find in traditional technical companies. It allows Google to innovate very, very quickly, which I think is a real strength of the company."

– Erick Schmidt, Former CEO Google

"We're not as prepared as we should be, as a government or as a country. From now on, communications networks and other digital infrastructure will be treated as they should be, as a strategic national asset."

– President Obama to the Wall Street Journal

"People don't usually wanna kill me for one of my movies until after they've paid 12 bucks for it."

–Seth Rogen, actor and producer regarding "The Interview" on Twitter,

1. Introduction

Warfare has influenced human affairs since the dawn of time, with warring factions struggling to gain a physical or geographic advantage today, the concepts encapsulated in communication synchronization offer a new realm of competition for this struggle. There is no more dynamic battle front than the cyber domain within communication synchronization. The Russian preemptive cyber-attacks on the Georgians, the Stuxnet virus that infected Iranian Nuclear Facilities, and the botnet attack on Estonia demonstrate the power and impacts of a weaponized cyber domain. Upon realizing the potential for cyber-warfare, international efforts and resources addressing this threat / capability have increased dramatically. In turn, international and national cyber strategies have been created to cope with the growing threats. The United States DoD created the Joint U.S. Cyber Command, with distinct component commands, to work along with other U.S. and Allied government agencies to address the threats in the cyber domain.

Understanding National and DoD communication synchronization concepts with the inherent strengths and limitations is the first step in examining the information domain. Then, students must be able to identify the threats, the ability to counter those threats, and ultimately what the value of those capabilities is to the military professional. Finally, students must comprehend the importance of cyber considerations in the planning process. Communication synchronization encompasses the entirety of the cognitive battlespace, and unlike its other components (information operations, space, and electronic warfare), cyber cannot be treated as just another

Marine Corps University / Command and Staff College
Warfighting / Complex Operational Problem Solving and Design

effects based tool of the fires process, rather cyber operations must be a consideration in each step of the planning process. The bottom-line is that commanders need to be aware of the importance of conducting cyber operations (CO) and planners must know how to incorporate them within the greater communication synchronization realm.

2. Student Learning Outcomes

1.3 Analyze the relationship between the Range of Military Operations (ROMO) and the spectrum of conflict.

2.3 Comprehend the global security environment and U.S. strategy and policy within their historical context.

2.4 Analyze joint and Marine Corps doctrine and emerging concepts, and their application within joint and multinational operations.

3.5 Analyze the dynamic interaction between cultures in conflict across the Range of Military Operations.)

4.5 Apply insights from history and other academic disciplines to enhance decision making.

7.4 Recognize the opportunities and vulnerabilities created by widespread information dissemination enabled by emerging media.

3. Supporting Educational Objectives

a. Discuss the capabilities and limitations of U.S. military forces to conduct offensive or defensive cyber operations across the full range of military operations. (CSC 1.3, 3.5; JPME 1a)

b. Explain cyber related guidance contained in strategic documents such as the national security strategy, the Quadrennial Defense Review, national military strategy, Defense Strategic Guidance. (CSC 2.3; JPME 1f)

c. Define the factors and emerging concepts such as cyber that have an influence on the development of joint doctrine. (CSC 2.4, 7.4; JPME 2b)

d. Explain and comprehend how information operations and cyberspace operations are integrated at the operational level. (CSC 2.4, 4.5, 7.4; JPME 4d)

e. Identify the role and perspective of the combatant commander and staff in developing offensive and defensive cyber operations plans associated with various theater level policies, strategies, and campaigns. (CSC 2.4; JPME 4g)

f. Identify the opportunities and vulnerabilities created throughout the range of military operations by reliance on networks and information technology in cyberspace. (CSC 1.3, 7.4; JPME 5c)

4. Student Requirements

Event	Prep
Contribute to Cyber Operations Seminar	1 hr
Required Reading: <ul style="list-style-type: none"> • Read Joint Publication 3-12(R) <i>Cyberspace Operations</i>, 5 February 2014. Executive Summary p. V; Chapter I, pp. II-16; Chapter II, pp. II1-II6; Chapter IV, pp. IV1-IV13. Blackboard • Read International Strategy For Cyberspace, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf Online • Read DOD <i>Strategy for Operating in Cyberspace</i>, July 2011. PP. 7-19 Blackboard 	68 PP

Marine Corps University / Command and Staff College
Warfighting / Complex Operational Problem Solving and Design

<ul style="list-style-type: none"> • Read Adam P. Liff (2012) “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War,” <i>Journal of Strategic Studies</i>, 35:3, 401-428, DOI: 10.1080/01402390.2012.663252 http://dx.doi.org/10.1080/01402390.2012.663252 Online • Read Vincent Manzo, “Deterrence & Escalation in Cross-Domain Operations: Where do Space and Cyberspace Fit?” <i>Strategic Forum, Institute for National Strategic Studies</i>, National Defense University, December 2011. Blackboard 	
<p>Supplemental Reading:</p> <ul style="list-style-type: none"> • Joint Publication 3-13-1 <i>Electronic Warfare</i>, 8 February 2012, Chapter I, pp. I-1 to I-17. Blackboard • Joint Publication 3-14 <i>Space Operations</i>, Chapter I, pp. I 1 to I 3. Blackboard • Marine Corps Order 3100.4, <i>Cyberspace Operations</i>, dated 27 July 2013, page 10. Blackboard • Joshua Davis, “Hackers Take Down the Most Wired Country In Europe” <i>Wired Magazine</i>, 15:09 (5 pages) http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1 Online • Lolita Boldor and Robert Burns, <i>Pentagon Discloses Massive Cyber Threat</i>, MSNBC, July 14, 2011 http://www.msnbc.msn.com/id/43757768/ns/technology_and_science-security/t/pentagon-discloses-massive-cyber-theft/from/toolbar Online • Stew Manuson, <i>Do Cyber Warriors Belong At Special Operations Command</i>, NDIA Magazine, August 2011 http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx Online • US DOD, Deputy Secretary Lynn’s Remarks, 16 June, 2011 http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4842 Online • Martin Libicki, <i>Cyberdeterrence and Cyberwar</i>, RAND Cooperation http://www.rand.org/pubs/monographs/MG877.html Online • Brookings Institution, 16 March 2011 http://www.brookings.edu/~media/Files/events/2011/0316_defense_challenges/20110316_defense_challenges_panel_2.pdf Online • Warwick Ashford, <i>How is Cyber Security Linked To Economic Security</i>, Computer Weekly.com, 31 May 2011 http://www.computerweekly.com/Articles/2011/05/31/246818/How-is-cybersecurity-linked-to-economic-security.htm Online 	
<p>Designated students should read <i>Marine Corps Intelligence Activity, Generic Intelligence Requirement Handbook, Information Operations/Information Warfare June 2003</i>, issued to MILFAC. This is an FOUO document and cannot be placed on BB. Chapter 5, pp. 70-74.</p>	

5. Issues for Consideration

- Define cyber, cyberspace, and Cyber Operations (CO).
- Are today’s commanders and staff officers prepared to conduct operational warfare in cyberspace? How do we operate and train in this domain?

Marine Corps University / Command and Staff College
Warfighting / Complex Operational Problem Solving and Design

- c. What is a hostile cyber act? What authorities does the President have both with and without a declaration of war?
- d. How do cyber threats impact the DoD?
- e. What are the similarities and the differences between cyberspace, space, and electronic warfare?
- f. How can DoD leverage other organizations and capabilities for 'fighting' in Cyberspace?
- g. What considerations should be made regarding cyber throughout the planning process?
- h. How do we include cyber operations in planning? How do they fit into an overarching communication synchronization plan?

6. Relationship to Other Instruction

The cyber curriculum will provide the student an understanding of the importance and the complexity of cyberspace and cyber operations. The student's understanding of our National Strategy for cyber, how other government agencies and civilian organizations address Cyberspace and the threats inherent therein, and cyber planning considerations will result in the students' ability to apply aspects of cyber to a greater communication synchronization plan during planning exercises.

7. References

- a. Commander's Communication Synchronization Plan JDN 2-13, 18 Dec 2014.
- b. International Strategy For Cyberspace, May 2011.

Lesson Hours:

Lecture	Guest Lecturer	Seminar discussion	Film	Practical Application	Staff Ride/Battle study	Evaluation/Test	TOTAL CONTACT HOURS	TOTAL SCHEDULE HOURS	Student Preparation Time	TOTAL HOURS
		2.0					2.0	2.0	3.0	5.0

JPME Data (JPME level):

Area 1						Area 2					Area 3						Area 4							Area 5			Area 6		
a	b	c	d	e	f	a	b	c	d	e	a	b	c	d	e	f	A	b	c	d	e	f	g	a	b	c	a	b	c
X					X		X													X			X			X			